Listen to What the Man Said\*: The Case for Amending the 3rd Party Doctrine for Home Recordings

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The 4th Amendment to the US Constitution requires law enforcement to obtain search warrants before conducting any unreasonable search and seizure of our homes, papers and effects. Technological changes over the years have required the Supreme Court to make judgments about how and when to apply this constitutional privacy protection over varying circumstances never contemplated by the Founders in the 1790’s.

Warrantless telephone wiretapping, for example, was allowed by a Supreme Court case in the 1920’s. But it was overturned by a later Court decision in the 1960’s (the *Katz* decision) , where the Court ruled that a citizen’s expectation of privacy was a large factor in determining the need for a search warrant, and that warrants would be required for government eavesdropping on phone calls.

Another factor is the “Third Party Doctrine.” The Supreme Court has ruled that, in general (with some new exceptions recently made), any information you voluntarily disclose to a “third party” (not yourself and not the government) is fair game for the government to collect without a warrant.

A classic example was the *Smith v. Maryland* case in 1979. Smith was arrested based in part on evidence collected by a tracking system activated at the state’s request (without a warrant) by the telephone company, which produced a list of the phone numbers his private home telephone had called. There was no wiretap and no eavesdropping on his phone calls. Smith argued his arrest violated the 4th Amendment because there was no search warrant. The Court ruled that by making phone calls, the information of who he was calling was automatically transmitted to the phone company, and Smith had to have known this, since it’s a condition of having telephone service. Since Smith had voluntarily given over his information to a “third party” (the phone company), he had no right to claim 4th Amendment protections, and no warrant was required.

Fast forward to the 21st century. Millions of American homes have “smart” devices that record various types of data, including actual voice conversations, in people’s homes. Every time you talk to Alexa or Siri or anyone like that, a server somewhere at Amazon or Google keeps a recording of that conversation (and no one knows for sure whether they are also recording “before” you say “Alexa!” or “Hey Siri!”). Since you voluntarily gave those personal assistants the right to record you in your home, and the recordings belong to “third parties”… they are not protected by the 4th Amendment. The government can demand the recordings from any of the service providers without a warrant. In effect, it’s like the government has a bug planted in millions of homes listening to conversations, completely bypassing the Constitution.

This case argues that the Supreme Court should extend 4th Amendment protection to recordings made inside the home by AI devices and remove them from the “Third Party Doctrine.”

\*#8 on Billboard, July 1975.

Listen to What the Man Said: Amending the 3rd party Doctrine 4

OBSERVATION 1. DEFINITIONS 4

Substantial 4

Reform 4

Artificial Intelligence 4

OBSERVATION 2. INHERENCY, the structure of the Status Quo. 4

FACT 1. The “Third Party Doctrine” 4

The Supreme Court says law enforcement doesn’t need a search warrant to obtain information you disclosed to others 4

FACT 2. Artificial Intelligence records household conversations 5

Personal assistants like Alexa record audio inside people’s homes and store the recordings on cloud storage 5

FACT 3. Constitutional law lags behind technology 5

Modern technology creates massive amounts of data vulnerable to privacy loss without 4th Amendment protection 5

OBSERVATION 3. The HARM. Invasion of the privacy of the home. We see this in 3 sub-points: 6

A. Massive exposure. Millions of private conversations are exposed to law enforcement 6

B. Not Hypothetical: Law enforcement has already started demanding warrantless access to home information 6

C. The Impact: Vital human rights are violated because the home deserves the utmost privacy protection 6

OBSERVATION 4. We need the following PLAN implemented by lower federal courts and the Supreme Court 7

OBSERVATION 5. SOLVENCY. Modifying the 3rd Party Doctrine is the answer. 7

Amending the 3rd Party Doctrine to give 4th Amendment protection for home devices will uphold privacy rights against unwanted intrusion 7

2A Evidence: 8

DEFINITIONS / TOPICALITY 8

Alexa and similar devices are “machine learning” technology 8

INHERENCY 8

A/T “Consumers can control privacy settings” 8

Some things cannot be controlled by the user. Others are too complicated and they don’t understand how to use them 8

Private information is shared from one tech company to another, and there’s no way to opt out 9

A/T “Status Quo court rulings” 9

Supreme Court hasn’t extended 4th Amendment to home data yet. But they should 9

Current Supreme Court rulings haven’t caught up with the current state of technology 9

HARMS / SIGNIFICANCE 10

A/T “Other things violate privacy too” – But privacy is not “all or nothing.” 10

Smart device recordings are as invasive to privacy as telephone wire tapping and should get the same 4th Amendment protection 10

Size of the problem is significant enough to justify granting 4th Amendment protection to smart device data. 10

Privacy is vital: Government eyes have no business prying into the intimate details of the home 11

Privacy in the home is a valuable fundamental human right that we must uphold 11

A/T “Users are voluntarily disclosing” – Advancing technology will pick up everything inside the home whether you disclose it or not 11

A/T “Users are voluntarily disclosing” – The 3rd Party Doctrine about voluntary disclosure is wrong because it’s built on circular reasoning 12

A/T “Consumers consent to exposure of their data” – They don’t know where it’s going, they don’t understand what’s being disclosed, and they can’t opt out. Such “consent” is meaningless 12

A/T “Voluntary disclosure” – The standard should be “reasonable expectation of privacy” regardless of disclosure 12

A/T “Privacy is dead, get over it” – Even privacy deniers must admit our homes and bedrooms deserve protection 13

SOLVENCY / ADVOCACY / ADVANTAGES 13

Supreme Court can and should modify its 4th Amendment rulings to protect home data 13

Third Party doctrine needs to evolve to keep up with technological challenges to 4th Amendment rights 13

Cell phone location data has been given 4th Amendment protection outside the 3rd Party Doctrine. Home device information should be treated the same way 14

We need new legal protections to update the 3rd Party Doctrine on smart device data 14

DISADVANTAGE RESPONSES 15

A/T “Warrant requirement slows/hampers police investigations” 15

Assumption that “requiring a warrant hampers law enforcement” is wrong because of the way criminals react to police tactics 15

Compromising 4th Amendment privacy protections doesn’t actually produce net benefits with law enforcement 15

Turn: 4th Amendment strengthens our security. Searching for a criminal needle in a haystack of data is easier when you stop adding more hay 16

Listen to What the Man Said: Amending the 3rd party Doctrine

The Fourth Amendment, which protects Americans from search and seizure without a warrant, upholds a vital human right in our society: the right to privacy. But the Supreme Court has recognized an exception to that protection in its so-called “Third Party Doctrine.” Whenever the citizen discloses information to someone else, the government doesn’t need a warrant to demand that “third party” hand over a copy of it. Modern day applications of Artificial Intelligence, combined with the Third Party doctrine, have created what amounts to a frightening new government bug listening in millions of American homes. That’s why we’re affirming that: The United States Federal Government should substantially reform the use of artificial intelligence technology.

OBSERVATION 1. DEFINITIONS

Substantial

Merriam Webster Online Dictionary copyright 2021. <https://www.merriam-webster.com/dictionary/substantially> (accessed 28 May 2021)

**:**considerable in quantity **:**significantly great

Reform

Merriam Webster Online Dictionary copyright 2021 <https://www.merriam-webster.com/dictionary/reform> (accessed 28 May 2021)

**:**to put or change into an improved form or condition

Artificial Intelligence

Merriam Webster Online Dictionary copyright 2021. <https://www.merriam-webster.com/dictionary/artificial%20intelligence> (accessed 28 May 2021)

**:**the capability of a machine to imitate intelligent human behavior

OBSERVATION 2. INHERENCY, the structure of the Status Quo.

FACT 1. The “Third Party Doctrine”

The Supreme Court says law enforcement doesn’t need a search warrant to obtain information you disclosed to others

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

Five years after the White decision, in United States v. Miller, the Court once again weighed in on third-party involvement in acquiring information and its effect on Fourth Amendment protection.[ **END QUOTE**] There, the Supreme Court upheld a district court ruling that convicted the defendant for conspiracy to defraud the United States of tax revenue on 175 gallons of whiskey. The Treasury Department subpoenaed the defendant’s bank records, stored by the bank in compliance with the Bank Secrecy Act, that pertained to business transactions to which the bank was privy. The defendant filed a motion to suppress some of his financial records obtained through subpoenas by investigators. The Supreme Court upheld the trial court’s denial of the defendant’s motion to suppress, reasoning that the Fourth Amendment did not apply because the documents were “negotiable instruments” containing voluntarily conveyed information, which were obtained through the bank’s ordinary course of business. [**SHE GOES ON LATER IN THE CONTEXT TO WRITE QUOTE:**] In Miller, the court articulated the third-party doctrine, stating that Fourth Amendment protections do not apply to information revealed to a third party and conveyed by the third party to government officials.

FACT 2. Artificial Intelligence records household conversations

Personal assistants like Alexa record audio inside people’s homes and store the recordings on cloud storage

Rebecca Levin 2019 (JD candidate, Univ. of Illinois College of Law) “Alexa, can you keep a secret?” An Analysis of 4th Amendment Protection Regarding Smart Home Devices University of *Illinois* Journal of Law, Technology & Policy 18 Feb 2019 <http://illinoisjltp.com/timelytech/alexa-can-you-keep-a-secret-an-analysis-of-4th-amendment-protection-regarding-smart-home-devices/> (accessed 11 Oct 2021)

Amazon’s Echo, commonly referred to as “Alexa,” is an artificial intelligence personal assistant that performs various tasks such as playing music, checking the weather or even buying goods from Amazon.com.  For Alexa to perform a task, the user must ask the device to do something such as play a song by saying the device’s “wake word” and then asking the device to perform a task. **[END QUOTE**]  For example, to play a song, a user may say, “Alexa, play Today’s Hits on Pandora.” While turned on and connected to the Internet, Alexa is always listening to her surroundings for a “wake word”, which is usually “Alexa” or another word chosen by the user.   Although Alexa is always listening to her surroundings, that does not mean the device is always recording and storing that data. Any kind of audio stated without a wake word is not sent to be stored on a server. **[SHE GOES ON TO SAY QUOTE:**] It is only when Alexa hears a wake word that audio from the fraction of the second before the wake word is spoken is recorded and sent to Amazon’s cloud to be processed.   After the audio with the wake word is sent and processed by Amazon’s cloud, Alexa responds appropriately to the user’s task, question or command.  Both the user’s command and Alexa’s response are archived in Amazon’s cloud.  In the example above, Amazon would process and then store the user’s command to play music on Pandora and then play the song on the device. Google’s device is similar to Amazon’s Echo in that the device answers factual questions, plays music and the radio, makes phone calls to others, and controls other electronic devices.   The Google Home device functions in a similar way to Amazon’s Echo device in that they listen for a wake word and begin recording from the very moment before that wake word is said.  This information is then stored in the Google cloud.

**END QUOTE. And keep in mind what I told you a moment ago, that the Supreme Court says you lose 4th Amendment protection for anything you disclose to someone else. All those recordings of everything going on in your home are now in someone else’s hands. That leads to…**

FACT 3. Constitutional law lags behind technology

Modern technology creates massive amounts of data vulnerable to privacy loss without 4th Amendment protection

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

Times have changed. And though the overarching idea of a smart home may seem feasible and desirable to consumers, ignorance of the complex systems underlying the technology leaves users vulnerable to cybersecurity risks and privacy infringement. Technological developments are outpacing corresponding regulation, and many forms of data records gathered from smart home technologies manufactured and managed by third parties are without Fourth Amendment protections. Because of the mass recording of metadata by technology companies such as Amazon, more data are being recorded, stored, analyzed, and transmitted to third parties than ever before.

OBSERVATION 3. The HARM. Invasion of the privacy of the home. We see this in 3 sub-points:

A. Massive exposure. Millions of private conversations are exposed to law enforcement

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

More than 100 million Alexa-equipped devices and 52 million Google Home devices have been sold globally as of early 2019. Of those Google Home devices, 43 million were installed in the United States. And as the devices become more popular, the privacy concerns are amplified—not only because more conversations are captured, but also because the dynamic of human interaction with smart home assistants evolves with their increasing adoption and technological advancement. Initially, people worried about the conversations smart home assistants might overhear. But the greater privacy threat posed by such devices, and the more useful data for law enforcement, may be the conversations users have directly with their digital assistants. For research purposes, I purchased an Amazon Echo device, and was surprised at the fluidity with which it (or “she,” as I’ve begun to reflexively call it/her) understands and responds to commands. The device engages in banter, intuitively digests complicated requests, and even has opinions. More than 50% of user interactions are “nonutilitarian”— seeking entertainment or companionship instead of the comparatively simple functionality for which Alexa is designed. It is no wonder, then, that in addition to asking Alexa to order an extra set of dryer sheets from Amazon, people have begun confiding in her in deeply personal ways, including sharing thoughts of suicide, experiences of abuse, and other private information. As Alexa gets smarter, more empathetic, and more human, we should expect her to learn increasingly intimate details about people’s inner lives—thoughts, feelings, and memories previously inaccessible to law enforcement except by interrogation, wiretapping, or undercover agents.

B. Not Hypothetical: Law enforcement has already started demanding warrantless access to home information

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

According to a transparency report from Nest Labs, Google’s smart home division that sells smart alarms, doorbells, thermostats, and cameras, governments have requested data from Nest on 300 occasions—affecting as many as 525 account holders—since 2015. Amazon, which received 1,955 government subpoena orders overall in the first half of 2019, has declined to publish the number of such requests made for Echo device data. Whatever the true number, it is clear that the government is becoming wise to the information-gathering potential of smart home devices.

C. The Impact: Vital human rights are violated because the home deserves the utmost privacy protection

Rebecca Levin 2019 (JD candidate, Univ. of Illinois College of Law) “Alexa, can you keep a secret?” An Analysis of 4th Amendment Protection Regarding Smart Home Devices University of *Illinois* Journal of Law, Technology & Policy 18 Feb 2019 <http://illinoisjltp.com/timelytech/alexa-can-you-keep-a-secret-an-analysis-of-4th-amendment-protection-regarding-smart-home-devices/> (accessed 11 Oct 2021) (brackets in original)

When determining whether or not one has a reasonable expectation of privacy, the Court has consistently held the home deserves the utmost protection under the Fourth Amendment.  In Silverman v. United States, the Court stated, “At the very core stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.”   Recently, in 2001, the Court reemphasized that notion in Kyllo v. United States, Justice Scalia writing for the majority stated, “[w]ith few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.”

OBSERVATION 4. We need the following PLAN implemented by lower federal courts and the Supreme Court

1. The Supreme Court will modify the “Third Party Doctrine” in all future cases to require Fourth Amendment protection for recordings made by artificial intelligence software in private homes. Search warrants will be required for law enforcement to obtain any such recordings from third parties.

2. No funding needed.
3. Enforcement through the lower federal courts and the Supreme Court. Any cases not in compliance will be reversed and retried following existing rules for the exclusion of evidence obtained without a proper warrant.
4. Plan takes effect the day after an affirmative ballot.
5. All Affirmative speeches may clarify

OBSERVATION 5. SOLVENCY. Modifying the 3rd Party Doctrine is the answer.

Amending the 3rd Party Doctrine to give 4th Amendment protection for home devices will uphold privacy rights against unwanted intrusion

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

In light of the introduction of novel smart home technologies to the consumer market, the manner in which Fourth Amendment protection extends to its users must evolve. In particular, privacy protections afforded to users ought to expand to the personal information stored by smart home devices in a company’s cloud. Courts need to adapt their interpretation and application of the third-party doctrine so that personal information disclosed to and recorded by smart home manufacturers and servers retains Fourth Amendment privacy protection. [**END QUOTE]** The Internet of Thing’s (IoT) novelty complicates application of past precedent in ensuring the privacy rights of users; although there are legislative measures in place to protect users from unwarranted search and seizure inside their home involving electronic devices, there is no statutorily recognized right to collect damages to remedy such intrusions. [**SHE CONTINUES IN THE SAME CONTEXT QUOTE**:] If courts can adapt their interpretation of the third-party doctrine to better fit into the changing technological environment and future on the horizon, the law will better protect each individual and ensure security from unwanted intrusion into the most intimate aspects of their life and home.

2A Evidence:

DEFINITIONS / TOPICALITY

Alexa and similar devices are “machine learning” technology

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

Smart home devices such as Amazon’s Alexa use real-time sensors that respond to unpredictable situations and requests, thus allowing users to converse with Alexa, interrogate Alexa, or even play games with Alexa. Although there is great potential benefit to be derived from IoT, the risks created by hastily released technologies coupled with unevolved regulations loom large. In the last thirty years, there has been a rapid increase in IoT innovation and a proliferation in development of smart home technologies aimed at increasing user convenience and efficiency. These new devices can gather and translate massive amounts of data and information about the homes they sit inside. One area of concern for users of smart home technology is their machine learning capabilities. Smart home systems can interact and combine, thus allowing these technologies to deduce relatively accurate and revealing personal data inferences about a user.

INHERENCY

A/T “Consumers can control privacy settings”

Some things cannot be controlled by the user. Others are too complicated and they don’t understand how to use them

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

Although Amazon’s Alexa is a helpful household assistant, it is also continuously collecting information without giving users the ability to withhold their consent and tell it to stop. Alexa’s competition, the Google Assistant, does not archive all recordings by default. Rather, it asks users whether or not they want to turn on audio recording settings, thus permitting Google to record audio after the wake-word (typically “hey Google”) is detected. This recording feature, however, is not automatically turned on and can be turned off by the user. When smart home technologies such as Alexa record all user interactions, whether intentional or mistaken, privacy concerns amass. Users often misunderstand the various data collection methods used by the smart home devices which inhibits consumers’ ability to reasonably and adequately evaluate privacy threats. Although Amazon’s privacy protocols require the company to maintain security safeguards when collecting and storing user information, there is little information available about what exactly those safeguards are. Amazon retains the right to not only keep a system of records tracking user interactions with the Alexa and other related information but also to provide certain third parties with the collected information.

Private information is shared from one tech company to another, and there’s no way to opt out

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

There are well-documented vulnerabilities common to many such devices that continue to be explored and documented by hackers and security organizations. But the greater concern is that even the most secure devices tend to store the data generated from within the home in “the cloud,” or on third-party servers. To make the problem worse, different manufacturers’ devices and cloud-based services often share data among themselves, increasing the number of parties with access to the web of information generated by smart devices within the home. Even when there is no overt cross-functionality, apps that run on smartphones, smart home assistants, and other smart home technology platforms reportedly share private data collected by the applications—from heart rate, to interest in buying a home, to whether the user is ovulating—with larger technology companies like Facebook, Amazon, Apple, or Google. Many of these apps share data with companies like Facebook whether or not the user is logged in via Facebook and without a way to opt out.

A/T “Status Quo court rulings”

 Supreme Court hasn’t extended 4th Amendment to home data yet. But they should

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

Most who have considered this issue have assumed smart home data stored on third-party servers, however intimate, lies outside the Fourth Amendment’s protection. Before Carpenter, the third-party doctrine was generally viewed as categorical, and often portrayed as such by the Court. In Carpenter, however, the Court dispelled the myth that the third-party doctrine sweeps so broadly. How and to what extent this move should and will reshape Fourth Amendment doctrine is an open question. I contend that Carpenter’s approach to bending the third-party doctrine in response to new technology opens the door to extending the Fourth Amendment’s protections to sensitive information stored on third-party servers, including smart home data. I also contend the Court did not go far enough and should abandon its “assumption of risk” approach to evaluating third-party doctrine cases.

Current Supreme Court rulings haven’t caught up with the current state of technology

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

In effect, the Court’s current approach would be to deny people Fourth Amendment protections because they have assumed the risk of adopting a technology until so many people have assumed the risk that the Court relents, adopting a fiction to declare the widespread, voluntary adoption of the technology nonconsensual.

HARMS / SIGNIFICANCE

A/T “Other things violate privacy too” – But privacy is not “all or nothing.”

Rebecca Levin 2019 (JD candidate, Univ. of Illinois College of Law) “Alexa, can you keep a secret?” An Analysis of 4th Amendment Protection Regarding Smart Home Devices University of *Illinois* Journal of Law, Technology & Policy 18 Feb 2019 <http://illinoisjltp.com/timelytech/alexa-can-you-keep-a-secret-an-analysis-of-4th-amendment-protection-regarding-smart-home-devices/> (accessed 11 Oct 2021)

While the Court decided the petitioner in Smith did not have a reasonable expectation of privacy in the phone numbers he called, the Court indicated that privacy was not an all or nothing principle.   Quoting Justice Marshall’s dissent from an earlier case, Cal. Bankers Association v. Shultz, the majority opinion in Smith stated, “Privacy is not a discrete commodity, possessed absolutely or not at all.  Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.”   Hence, merely because someone gives up their right to privacy by disclosing their phone number, it does not mean the communications of that phone are not private.  In the context of smart home devices, this means that simply because users consent to Amazon and Google having access to their location, it does not mean they give up their right to privacy in what music they listen to or what information they ask their devices.  However, it does mean that by storing information on servers, users would seem to forfeit their right to privacy with what is on those servers.  For Amazon users and their devices, this means that whatever commands they ask of their device, as well as their device’s responses, are not private.

Smart device recordings are as invasive to privacy as telephone wire tapping and should get the same 4th Amendment protection

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)(“Katz” refers to the 1967 Supreme Court decision requiring search warrants for wiretapping a public telephone)

The invasiveness of searching smart home device data is plain. Smart homes open a window into people’s private lives as large as or larger than each technology to which the Court has already extended Fourth Amendment protection. In Katz, the Court was concerned about the police capturing private phone conversations made in public telephone booths.

Size of the problem is significant enough to justify granting 4th Amendment protection to smart device data.

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

The growing adoption of smart home devices provides additional reason to extend Fourth Amendment protections to the data they generate. It is projected that 20% of households will own smart devices by 2022, and nearly 60% of Americans want them. Already, more than 66 million adults are estimated to own smart speakers, including a 40% increase in ownership in 2018 alone. Two-thirds of Americans are forecast to own a smart speaker by 2022. And new homes are being built with these devices pre-installed. If they haven’t already, smart home devices are poised to permeate modern society, taking on an increasingly large role in modern life. To withhold Fourth Amendment protection from the data they generate would be to ignore the “vital role” they do and will play in society.

Privacy is vital: Government eyes have no business prying into the intimate details of the home

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021) (“Kyllo” refers to the 2001 Supreme Court case Kyllo v. U.S., where the Court ruled that agents stationed outside the home with a thermal imaging device measuring heat generated by his indoor marijuana farm had violated the 4th Amendment, even though they never went on Kyllo’s property)

In addition to emphasizing the historical primacy of the home and the need to construe the Fourth Amendment sufficiently flexibly to keep pace with advancing technology, the *Kyllo* Court manifested a belief that the home is a place of special intimacy worthy of expansive privacy protections. “In the home,” the Court wrote, “all details are intimate details, because the entire area is held safe from prying government eyes.” Setting aside the circularity of inferring that homes must be private because they are entitled to privacy, the Court’s language evokes concern about the way that police observation of even ostensibly innocuous details emanating from people’s homes may reveal deeply personal portraits of their lives

Privacy in the home is a valuable fundamental human right that we must uphold

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021) (brackets and ellipses in original)

For the Supreme Court, the home is sacred. It is at the “core of the Fourth Amendment.” Police may not enter a home, arrest a suspect at home, move a stereo inside a home to look underneath it, have a dog sniff the outside of a home, or point a thermal imager at a home without a warrant and probable cause. In the words of Stephanie Stern: “Homes have achieved iconic status in the modern Fourth Amendment, with judicial rhetoric elevating residential search to the apex of protection.” The primacy of the home in Fourth Amendment jurisprudence is explained in part by its explicit inclusion in the text of the Fourth Amendment, whose vagaries otherwise frustrate scholars and Justices alike. The Fourth Amendment provides, in relevant part: “The right of the people to be secure in their . . . houses . . . shall not be violated . . .” No test need be devised to divine the unambiguous commandment of our Founding Fathers that “[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.” The history points in the same direction. In a 1763 address in the House of Commons, William Pitt proclaimed:
The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement!

A/T “Users are voluntarily disclosing” – Advancing technology will pick up everything inside the home whether you disclose it or not

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

A formalistic distinction between physical penetration of the home and surveillance through information that escapes the home’s physical limits “would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home.” Any other finding would lead to a slippery slope that would end in the Court blinking as “ultrasound technology produces an 8-by10 Kodak glossy.

A/T “Users are voluntarily disclosing” – The 3rd Party Doctrine about voluntary disclosure is wrong because it’s built on circular reasoning

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021) (brackets in original) (“Carpenter” refers to the 2018 Supreme Court case of Carpenter v. United States, where the Court ruled against allowing warrantless law enforcement searches of cell phone location tracking)

The third-party doctrine may be the most reviled Fourth Amendment canon. Voluntary disclosure decisions “top[] the chart of [the] most-criticized [F]ourth [A]mendment cases.” As Orin Kerr put it, “[a] list of every article or book that has criticized the doctrine would make [for] the world’s longest law review footnote.” The panning has only intensified as scholars recognized “[t]he third-party doctrine [as] one of the most serious threats to privacy in the digital age.” Even before Carpenter, the Court has declined to offer much defense for the doctrine beyond asserting that those who share information with a third party “assume[] the risk” that it will end up in the wrong hands. Of course, that rationale is circular. There would be no risk to assume if the law continued to protect the information after its disclosure.

A/T “Consumers consent to exposure of their data” – They don’t know where it’s going, they don’t understand what’s being disclosed, and they can’t opt out. Such “consent” is meaningless

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021) (the last sentence about it being the same as transmitting location data is a reference to the Carpenter v. United States 2018 decision, where the Supreme Court ruled against warrantless searches of cell phone location data, even though phone users “voluntarily” know that their phone is pinging off cell towers and giving away their location)

The smart home also demonstrates the patent unfairness of punishing people for adopting consumer technologies that undermine their privacy in ways they cannot and do not understand. To the extent consumers understand that purchasing useful gizmos for their home constitutes voluntary disclosure of their most sensitive data to a third party, they may not know the path their data will follow because of companies’ opaque data-sharing policies. In many cases, apps share exceedingly private data with other companies without a way for the user to opt out. It defies reality to suggest that people consent to such third-party disclosure more meaningfully than to the transmission of their location directly to their cell phone service provider.

A/T “Voluntary disclosure” – The standard should be “reasonable expectation of privacy” regardless of disclosure

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021) (“Katz” refers to the 1967 Supreme Court case Katz v. United States, where the Court ruled that warrantless wiretapping of a public phone booth was a violation of the 4th Amendment because its users had an “expectation of privacy”)

The Court has recognized since Katz that people have a reduced expectation of privacy over information knowingly disclosed to third parties or the public. Indeed, in many cases, the privacy interests implicated by a category of technology measured against the voluntariness of people’s data disclosure will militate against extending Fourth Amendment protection. But to categorically refuse to apply the Fourth Amendment when the disclosure was voluntary is illogical and devastating to privacy in modern society. It should be sufficient to demonstrate that an individual maintained an objectively reasonable expectation of privacy over the information despite voluntarily disclosing it to a third party.

A/T “Privacy is dead, get over it” – Even privacy deniers must admit our homes and bedrooms deserve protection

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021) (brackets in original)

Privacy scholars and science fiction authors alike have viewed technology with suspicion for decades. To many, the rise of consumer technology and the surveillance state signals the end of days for any meaningful sense of privacy. As a prominent technology CEO infamously put it in 1999: “You have zero privacy anyway. Get over it.” Some scholars have set out to develop a theory of the Fourth Amendment untethered to the concept of privacy, reflecting “a world without privacy.” Perhaps the most influential death-of-privacy prognosis came from futurist David Brin. In The Transparent Society, Brin argued forcefully that our attempts to salvage privacy are doomed: “[I]t is already far too late to prevent the invasion of cameras and databases. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay.” But even Brin, among the fiercest of privacy doomsday theorists, did not anticipate private or government surveillance reaching into the home. Even in the most extreme world of surveillance Brin could imagine, people would retain a baseline level of “bedroom privacy.” Even as “camera-bearing robots may swarm the skies,” there will remain “a realm that each of us calls deeply personal, wherein we seek either solitude or intimacy.” That is, a “place to hold things we want kept private.”

SOLVENCY / ADVOCACY / ADVANTAGES

Supreme Court can and should modify its 4th Amendment rulings to protect home data

Gabriel Bronshteyn 2020 (JD candidate, Stanford Law School) Feb 2020 STANFORD LAW REVIEW Searching the Smart Home <https://review.law.stanford.edu/wp-content/uploads/sites/3/2020/02/Bronshteyn-72-Stan.-L.-Rev.-455.pdf> (accessed 12 Oct 2021)

Setting aside the specific doctrinal tests the Court may employ, the answer to the broader legal question—whether smart home data is entitled to Fourth Amendment protection—should be “yes.” The Court has demonstrated that the contours of the Fourth Amendment are subject to change, especially when new technologies reshape the dynamic between people and police. Here, the profound intimacy of the data generated by smart home devices, the impending ubiquity of their adoption, and the ease and scope of the surveillance they enable compels Fourth Amendment protection.

Third Party doctrine needs to evolve to keep up with technological challenges to 4th Amendment rights

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum 24 June 2021 <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

Each day brings forth new innovations. It is important that the laws and regulations adapt and evolve with the technologies to maximize consumer protection. The Fourth Amendment affords individuals a right to privacy in their person and protects them from unreasonable searches and seizures. The third-party doctrine is an exception to this protection, where consumers lose their right to privacy for information voluntarily disclosed to another. With the introduction and implementation of the Internet of Things, new concerns arise over the Court’s usage of the third-party doctrine and consumers’ Fourth Amendment rights. Ultimately, the Court will have to adapt its application of the long-standing third-party doctrine to ensure that technological innovation does not undermine users’ Fourth Amendment protections.

Cell phone location data has been given 4th Amendment protection outside the 3rd Party Doctrine. Home device information should be treated the same way

Rebecca Levin 2019 (JD candidate, Univ. of Illinois College of Law) “Alexa, can you keep a secret?” An Analysis of 4th Amendment Protection Regarding Smart Home Devices University of *Illinois* Journal of Law, Technology & Policy 18 Feb 2019 <http://illinoisjltp.com/timelytech/alexa-can-you-keep-a-secret-an-analysis-of-4th-amendment-protection-regarding-smart-home-devices/> (accessed 11 Oct 2021)

As the analysis above suggests, smart home device users are not protected by the Fourth Amendment under current case law because access to the information they possess is not considered a traditional search or seizure, and does not implicate the protections of the Fourth Amendment.  While the Fourth Amendment traditionally provided the utmost protection for the home, given the Third-Party Doctrine, is unclear whether it is reasonable to expect privacy when using smart devices in one’s home given third parties have access to this information per the terms of agreement users accept when using home smart devices.  In Carpenter, the Court held the Third-Party doctrine did not apply because cell phone location data is able to provide a complete profile on someone including not only their whereabouts but also whom they associate with.   Like cell phone location data, smart home device data also contains this kind of deeply personal information such as what music one listens to and what books and articles they read.  Given the similarities between the data, smart home device information should be afforded the same protection as cell phone location data and the Third-Party Doctrine should also not apply in the case of smart home devices.

We need new legal protections to update the 3rd Party Doctrine on smart device data

Katherine Minorini 2021 (J.D. Candidate, Boston College Law School) A VENDETTA AGAINST ALEXA: PRIVACY CONCERNS IN THE AGE OF THE SMART HOME, Boston College Intellectual Property & Technology Forum 24 June 2021 <http://bciptf.org/wp-content/uploads/2021/06/Minorini_Vendetta-Against-Alexa_2021-.pdf> (accessed 11 Oct 2021)

With the advent of IoT, courts should not apply past interpretations of the third-party doctrine to automated transactions or to information disclosed to smart home devices. Rather, in such circumstances, courts should interpret the third-party doctrine more in line with the Technosocial Theory, which would provide users better protection in their homes. Further, the Court should hold smart home device manufacturers accountable if they fail to protect user information and data voluntarily conveyed to a home assistance device. Congress has already acknowledged a need for regulation and control in the federal agencies, citing security concerns as its justification. Although the onus is on the manufacturers creating these technologies to ensure the metadata is secure, the Court must hold them accountable for securing and protecting the massive amount of data they continue to collect on unknowing commercial users. As a starting point, courts should establish boundaries of what information can be conveyed to third parties as a part of business transactions, ensuring that the information transferred is not unique to the user nor revealing of their private life.

DISADVANTAGE RESPONSES

A/T “Warrant requirement slows/hampers police investigations”

Assumption that “requiring a warrant hampers law enforcement” is wrong because of the way criminals react to police tactics

Prof. Tonja Jacobi and Jonah Kind 2015. (Jacobi - Professor, Northwestern University School of Law. - Kind - Law Clerk to the Honorable Joel M. Flaum, U.S. Court of Appeals, Seventh Circuit) WILLIAM & MARY LAW REVIEW 15 Feb 2015 CRIMINAL INNOVATION AND THE WARRANT REQUIREMENT: RECONSIDERING THE RIGHTS-POLICE EFFICIENCY TRADE-OFF <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=3574&context=wmlr> (accessed 14 Oct 2021) (brackets added)

We challenge the assumption that requiring LEOs [Law Enforcement Officers] to obtain a warrant prior to undertaking a particular action will always make law-enforcement investigations and prosecutions more difficult. Often, perhaps even usually, not needing a warrant will be better for law enforcement for obvious reasons: officers must expend time and effort to obtain the warrant; the warrant process may create delays that allow for the destruction or concealment of evidence; and having to show probable cause to obtain the warrant means that some investigations will be blocked altogether. However, because criminals can innovate, the assumption of greater law-enforcement efficiency in the absence of the warrant requirement can be wrong. When LEOs do not need a warrant, they will be more likely—all other things being equal—to investigate because the costs of investigation are lower. However, this lowered cost of investigation will incentivize criminals to innovate more often because innovations lower the likelihood of detection in the event of law-enforcement.

Compromising 4th Amendment privacy protections doesn’t actually produce net benefits with law enforcement

Prof. Tonja Jacobi and Jonah Kind 2015. (Jacobi - Professor, Northwestern University School of Law. - Kind - Law Clerk to the Honorable Joel M. Flaum, U.S. Court of Appeals, Seventh Circuit) WILLIAM & MARY LAW REVIEW 15 Feb 2015 CRIMINAL INNOVATION AND THE WARRANT REQUIREMENT: RECONSIDERING THE RIGHTS-POLICE EFFICIENCY TRADE-OFF <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=3574&context=wmlr> (accessed 14 Oct 2021) (brackets added)

The reasonable expectation of privacy test has been derided as circular because an expectation of privacy will depend on the extent to which police regularly breach that expectation; moreover, expectations of privacy will depend on legal decisions, which are supposed to be based on people’s expectations of privacy. This circularity can lead to a spiral of ever-decreasing Fourth Amendment rights whereby increased government surveillance erodes people’s privacy expectations, making the surveillance legal under the test. Though such a downward spiral decreases the rights of everyone, including non-criminals, it is usually considered at least to have the beneficial effect of making it easier for law enforcement to catch criminals. Our analysis, however, demonstrates that this advantage will often be illusory. LEOs [Law Enforcement Officers] will often not have an easier time catching criminals because increased surveillance may simply result in increased criminal innovation. In the cat-and-mouse game between law enforcement and criminals, the reasonable expectation of privacy test will erode the rules of the game without making it easier for the cat to catch the mice; meanwhile, innocent bystanders will receive less Fourth Amendment protection.

Turn: 4th Amendment strengthens our security. Searching for a criminal needle in a haystack of data is easier when you stop adding more hay

**[Analysis: The “needle” is the incriminating evidence. The “hay” is all the millions of conversations you’re collecting that have no value. Without a warrant you collect millions more and it’s mostly hay. If you require probable cause, it forces law enforcement to focus only on those that are likely to have some evidentiary value, rather than just collecting everything and then having to sift through it all.]**

Norman Solomon 2015 (executive director of the Institute for Public Accuracy ) 26 Aug 2015 “Why government surveillance won’t protect your data” FORTUNE magazine <https://fortune.com/2015/08/26/cybersecurity-nsa-att/> (accessed 14 Oct 2021)

But far from being legalistic antiques that have outlived their usefulness in our modern era of terrorism, the Fourth Amendment’s requirements for “probable cause” and specificity of warrants are not only matters of bedrock constitutional principle. They also enhance our security. Adherence to the Fourth Amendment — with its insistence on targeted rather than general warrants — actually provides much better protection against terrorism than aiming the government’s digital blunderbuss at millions of people. Former FBI special agent Coleen Rowley, who was a [Time magazine](http://content.time.com/time/specials/packages/0%2C28757%2C2022164%2C00.html) “Person of the Year” in the wake of 9/11, [points out](http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks) that mass surveillance makes preventing terrorism and catching bad guys less — not more — likely. If locating terrorist plotters is akin to finding a needle in a haystack, Rowley insists, the last thing we should do is keep adding more hay.